Logging file changes for Incremental and Differential Images

Your Windows operating system and installed applications can create many changes 'under the hood' without you knowing about it. This can cause Incremental or Differential images to be substantially larger than expected. This article describes a feature in Macrium Reflect to log files that have been changed in each Incremental or Differential image.

Note: In Macrium Reflect v7, this functionality is only available if Changed Block tracker (CBT) s disabled. Take **'Other Tasks' > 'Edit Defaults' > 'Advanced' > 'Advanced Incrementals'** and **un-check 'Enable Changed Block Tracker'**

What are Incremental and Differential Images?

Incremental images will only backup data blocks that have changed since the last Image or, in the case of Differential, Full image in the backup set. Images are created at File System cluster level and each block is MD5 hashed and compared. Blocks with the same hash signature aren't included in the Differential or Incremental image file. A data block is usually 16 clusters in length.

See also: How backup sets are created and maintained

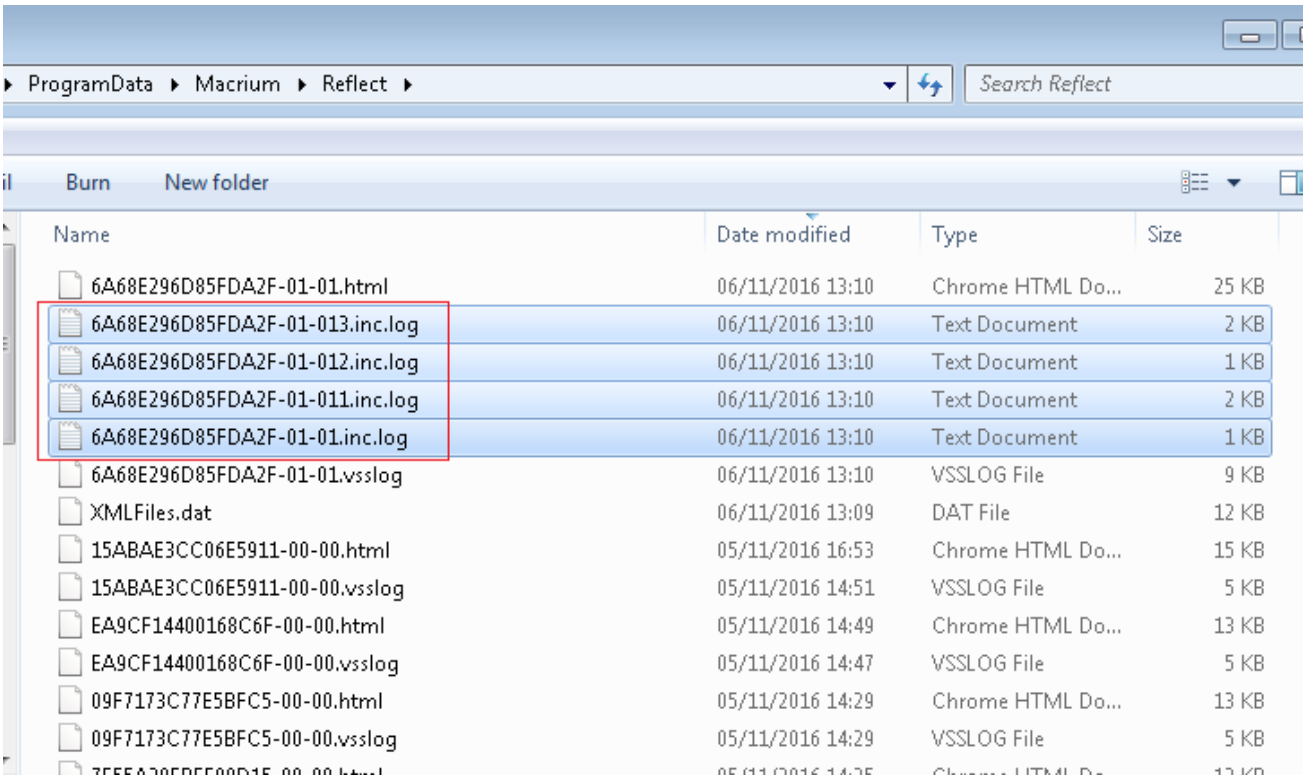
How to show changed files

If the following registry entry is set, Reflect will perform a reverse 'look-up' to identify the file for each cluster that is backed up.

This may increase the time taken to backup and **should only be used for diagnosis.**

Key:	HKEY_LOCAL_MACHINE\SOFTWARE\Macrium\Reflect\Settings
Name:	LogIncrementalChanges
Type:	DWORD
Value:	1

Once the registry entry is set, **perform another Differential or Incremental Image** and, once complete, **delete the registry entry created above**. Then use Windows Explorer to **navigate to: 'C:\ProgramData\Macrium\Reflect'** in Windows Explorer and **sort by Modified Date**:



In addition to the normal '.html' and '.vsslog' files you will also see files with '.inc.log' at the end. There will be one for each NTFS partition in the Differential or Incremental.

The first file, **{IMAGEID}-XX-YY.inc.log,** is the log for the first NTFS partition, the next file is , **{IMAGEID}-XX-YY1.inc.log** and,

in the above example, **{IMAGEID}-XX-YY3.inc.log** is the last last NTFS partition in the image.

Example log output

```
MFT Record - 32 - .\$Extend\$RmMetadata\$TxfLog\$TxfLog.blf
MFT Record - 34 - .\$Extend\$RmMetadata\$TxfLog\$TxfLogContainer00000000000000000002
MFT Record - 38 - .\Windows\Prefetch\AgGlGlobalHistory.db
MFT Record - 39 - .\Windows\Prefetch\AgGlFaultHistory.db
MFT Record - 43 - .\Windows\Prefetch\AgRobust.db
MFT Record - 45 - .\Windows\Prefetch\AgGlFgAppHistory.db
MFT Record - 1236 - .\Windows\SoftwareDistribution\SelfUpdate\WuPackages.xml
MFT Record - 1333 - .\Program Files (x86)\TeamViewer\Version8\TeamViewer8_Logfile.log
MFT Record - 1353 - .\ProgramData\Microsoft\RAC\PublishedData\RacWmiDatabase.sdf
MFT Record - 1592 - .\Users\Dev\AppData\Local\Google\Chrome\User Data\Default\Current Session
MFT Record - 1783 - .\Program Files\Microsoft SQL Server\MSSQL10.SQLEXPRESS\MSSQL\Log\ERRORLOG
MFT Record - 13900 - .\Windows\System32\winevt\Logs\Microsoft-Windows-PrintService%4Admin.evtx
MFT Record - 15637 - .\Windows\WindowsUpdate.log
MFT Record - 15741 - .\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender%4Operational.evtx
MFT Record - 15743 - .\Windows\System32\winevt\Logs\Microsoft-Windows-Windows Defender%4WHC.evtx
MFT Record - 15755 - .\Users\Dev\AppData\Local\Google\Chrome\User Data\Default\IndexedDB\http_localhost_2904.
indexeddb.leveldb\LOG
MFT Record - 15868 - .\Windows\bootstat.dat
MFT Record - 21541 - .\Windows\security\database\secedit.sdb
MFT Record - 21544 - .\Windows\ServiceProfiles\LocalService\NTUSER.DAT
MFT Record - 21565 - .\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
MFT Record - 22562 - .\Windows\ServiceProfiles\NetworkService\AppData\Local\Temp\MpCmdRun.log
MFT Record - 22649 - .\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-1.C7483456-A289-439d-8115-
601632D005A0
MFT Record - 22650 - .\Windows\System32\7B296FB0-376B-497e-B012-9C450E1B7327-5P-0.C7483456-A289-439d-8115-
601632D005A0


And so on.........
```

Each log file lists the MFT record and full path name to the file(s) that have changed.

There will be many MFT metadata files (prefixed by '$') that are not visible to Windows Explorer or any other windows utilities, but these are always included (if changed) in Diff/Inc image files.
Please note that this doesn't mean that all clusters in the listed files have changed it means that the file clusters are scanned and differences have been detected.